Vandiver予想と正規底について(代数的整数論とその周辺)

AUTHOR(S):

小松, 啓一

CITATION:

小松, 啓一. Vandiver予想と正規底について(代数的整数論とその周辺). 数理解析研究所講究録 1998, 1026: 12-19

ISSUE DATE:

1998-02

URL:

http://hdl.handle.net/2433/61774

数理解析研究所講究録
1026巻 1998年 12-19

Vandiver 予想と正規底について

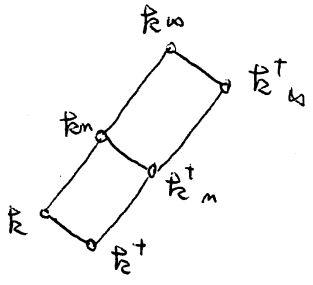
早大理工 小松啓一 (Keiichi Komatsu)

正の整数 n に対して，$\zeta_n = e^{\frac{2\pi i}{n}}$ とし，奇素数 p に対して，$k = \mathbb{Q}(\zeta_p)$ とし，k^+ を k の最大実部分体，h_{k^+} を k^+ の類数とする。このとき p が h_{k^+} を割らないというのが Vandiver 予想である。さらに k の cyclotomic $\mathbb{Z}_p$-拡大を k_∞ とする。この場合 $k_\infty = k(\{\zeta_{p^m} ; \mathbb{Z} \ni m > 0\})$ となり $G(k_\infty/k) \simeq \mathbb{Z}_p$ となっている。k^+ の cyclotomic $\mathbb{Z}_p$-拡大を k^+_∞ とすると

$$k^+ = k^+_0 \subset k^+_1 \subset \cdots \subset k^+_m \subset \cdots \subset k^+_\infty$$

$$G(k^+_m/k^+) \simeq \mathbb{Z}/p^m\mathbb{Z}$$

となる拡大体の列が存在する。



さらに A^+_m を k^+_m のイデアル類群の p-part とすれば，岩沢の定理により，0以上の整数 $\lambda(k^+)$ と $\mu(k^+)$ および整数 $\nu(k^+)$ があり

$$\#A^+_m = p^{\lambda(k^+)m + \mu(k^+)p^m + \nu(k^+)}$$

が十分大きなnに対して成立する。ただし $\#A_m^+$ は A_m^+ の位数を表すとする。このとき Ferrero - Washington [ ] により，$\mu(\mathfrak{p}^+)=0$ がしられている。一方 Greenberg により $\lambda(\mathfrak{p}^+)=0$ が予想されている。pが $h_{\mathfrak{p}^+}$ を割らないならば $\lambda(\mathfrak{p}^+)=0$ であることを注意しておく。

さて，自然数 $n \leqq m$ について A_m^+ から A_m^+ への自然な準同型があるが，それについての $\{A_m^+\}$ の inductive limit を $\varinjlim_m A_m^+ = A_\infty^+$ とする。このとき，

$\lambda(\mathfrak{p}^+)=0 \iff A_\infty^+=0 \iff$ 任意の自然数 n と A_n^+ の任意の元 a について，a に属するイデアルは n より十分大なる m について $\mathfrak{p}_m^+$ で単項化する。

$\mathbb{Q}_{ab}=\mathbb{Q}(\{\zeta_n : \mathbb{Z}\ni n>0\})$，$\mathbb{Q}_{ab}^+$ を $\mathbb{Q}_{ab}$ の最大実部分体 Kを $\mathbb{Q}$ の有限次拡大体，C_K をKのイデアル類群とする。

$$C_{\mathbb{Q}_{ab}^+} = \varinjlim_{\substack{\mathbb{Q}_{ab}^+ \supset K \\ (K:\mathbb{Q})<\infty}} C_K \qquad \text{とする。}$$

このとき M. Kurihara [7] は次のような興味深い結果を得た。

Theorem 1. $C_{\mathbb{Q}_{ab}^+}$ は trivial である。

この定理は $\mathfrak{p}_m^+$ のイデアルは $\mathbb{Q}_{ab}^+$ の十分大きな有限次

部分体で単項化していることをいっており，Greenberg 予想と比較して大変興味深い結果である。一方 $C_{\mathbb{Q}^{ab}}$ は大変大きな群になっていることを注意しておく。

次に $\mathbb{Z}_p$ - 拡大の正規 - p - 基底と Vandiver 予想との関係について述べることにする。k を有限次代数体 K を k の $\mathbb{Z}_p$ - 拡大とし，

$$k=K_0 \subset K_1 \subset \cdots \subset K_m \subset \cdots \subset K \qquad (K_m : k)=p^m$$

とする。

Def. $\mathbb{Z}_p$ - 拡大 K/k が正規 - p - 基底を持つ。
$\overset{\text{def.}}{\Longleftrightarrow}$ 任意の自然数 m に対して，$\mathcal{O}_{K_m}[\frac{1}{p}]$ の元 θ_m があって $\{\theta_m^{\tau}\}_{\tau \in G(K_m/k)}$ が $\mathcal{O}_{K_m}[\frac{1}{p}]/\mathcal{O}_k[\frac{1}{p}]$ の基底になっている。

このとき次の定理が成立する。

Theorem 2 (cf. [4]) p を奇素数，$\zeta_p=e^{\frac{2\pi i}{p}}$，$k=\mathbb{Q}(\zeta_p)$ $k^+=k\cap\mathbb{R}$，h_{k^+} を k^+ の類数とする。このとき次は同値

(1) p は h_{k^+} を割らない。

(2) $\lambda(k^+)=0$ で k の $\frac{p+1}{2}$ この独立な $\mathbb{Z}_p$ - 拡大がすべて正規 - p - 基底をもつ。

上の定理から Vandiver予想の研究にとって $\mathbb{Z}_p$-拡大の正規-p-基底の研究が大切であることがわかる。これについて以下に述べる事が知られている。

Prop. 1. (cf. [3]) k を有限次代数体，k_∞ を k の cyclotomic $\mathbb{Z}_p$-拡大とする。このとき k_∞/k は正規-P基底をもつ。

Prop. 2. (cf. [2], [5]) k を虚2次体，$\tilde{k}$ を k の絶対類体，K を k の $\mathbb{Z}_p$-拡大，このとき $p \neq 3$ ならば，$K\tilde{k}/\tilde{k}$ は正規-p-基底をもつ。

Prop. 2より次がわかる。

Prop. 3. $p \equiv 3 \pmod 4$ $p \neq 3$, $(\mathbb{Q}(\sqrt{-p}) \subset \mathbb{Q}(\zeta_p)$ とする) K を $\mathbb{Q}(\sqrt{-p})$ の $\mathbb{Z}_p$-拡大とすれば，$K\mathbb{Q}(\sqrt{-p})/\mathbb{Q}(\sqrt{-p})$ は正規-P-基底をもつ。

Prop. 2 の証明には，modular units がもちいられる。このことから，次の問題を考えることは意味があるように思われる。

問題 虚アーベル体のアーベル拡大の正規底や単数を Siegel modular 関数の特殊値でどのぐらい構成できるか。

以後 $\zeta = e^{\frac{2\pi i}{5}}$, $k = \mathbb{Q}(\zeta)$, 正の整数 m に対して, $k(m)$ で k の mod m の ray class field を表すとする。さらに $S_m = \{ a \in k^\times ; \ a \equiv 1 \pmod{m} \}$, $\widetilde{S}_m = \{ (a) : a \in S_m \}$

$G(k/\mathbb{Q})$ の元で $\zeta^\alpha = \zeta^2$ となるものを固定し, $k^\times$ の自己準同型 φ を $\varphi(a) = a^{1+\alpha^3}$ $a \in k^\times$ で定める。さらに U を k の単数群とする。このとき,

$$G(k(2p^2)/k(2p)) \cong \widetilde{S}_{2p}/\widetilde{S}_{2p^2} \cong S_{2p}/S_{2p^2}(S_{2p} \cap U)$$

となる。 $H = S_{2p^2}(S_{2p} \cap U)$ とおけば, $\varphi(H) \subset H$ となり,

準同型 $\widetilde{\varphi} : S_{2p}/H \to S_{2p}/H$ が $\widetilde{\varphi}(aH) = \varphi(a)H$

により induce される。このとき $\widetilde{\varphi}(S_{2p}/H) \cong (\mathbb{Z}/p\mathbb{Z})^3$ がわかり, $\operatorname{Ker}\widetilde{\varphi}$ に対応する類体を L とすれば,

$$G(L/k(2p)) \cong (\mathbb{Z}/p\mathbb{Z})^3$$

となる。

$\mathfrak{H}_2 = \{ \tau \in M_2(\mathbb{C}) ; \ {}^t\tau = \tau, \ \operatorname{Im}\tau \text{ is positive definite} \}$

を degree 2 の Siegel 上半空間とする。さらに,

$$\tau_0=\frac{1}{5}\begin{pmatrix} 2+\zeta-\zeta^2-2\zeta^4 & 2-\zeta+\zeta^2-2\zeta^3 \\ 2-\zeta+\zeta^2-2\zeta^3 & \zeta+2\zeta^2-2\zeta^3-\zeta^4 \end{pmatrix} \quad \text{とおけば},$$

τ_0 は $\mathfrak{H}_2$ の点で，$y^2=1-x^5$ の principal polarization をもった Jacobian variety にふさいした CM-point となる。

複素数 t に対して，$e(t)=e^{2\pi i t}$，$\tau\in\mathfrak{H}_2$，$\kappa=\begin{pmatrix}\kappa_1\\ \kappa_2\end{pmatrix}\in\mathbb{R}^2$，$\lambda=\begin{pmatrix}\lambda_1\\ \lambda_2\end{pmatrix}\in\mathbb{R}^2$，$u=\begin{pmatrix}u_1\\ u_2\end{pmatrix}\in\mathbb{C}^2$ とし，テータ関数を

$$\Theta(u,\tau;\kappa,\lambda)=\sum_{x\in\mathbb{Z}^2} e\left(\frac{1}{2}{}^t(x+\kappa)\tau(x+\kappa)+{}^t(x+\kappa)(u+\lambda)\right)$$

とおき，

$$\Psi(\tau;\kappa,\lambda)=\frac{2\Theta(0,\tau;\kappa,\lambda)}{\Theta(0,\tau;0,0)} \qquad \text{とおく。}$$

然らば，正の整数 N に対して，$\kappa,\lambda\in\frac{1}{N}\mathbb{Z}^2$ のとき，$\Psi(\tau;\kappa,\lambda)$ はレベル $2N^2$ の Siegel modular function となる。このとき次の定理が得られる。

Theorem 3 ([6]) $\Psi_1(\tau_0)=\Psi(\tau_0;\begin{pmatrix}\frac{1}{p}\\ 0\end{pmatrix},\begin{pmatrix}0\\ 0\end{pmatrix})$，
$\Psi_2(\tau_0)=\Psi(\tau_0;\begin{pmatrix}\frac{1}{p}\\ 0\end{pmatrix},\begin{pmatrix}\frac{1}{p}\\ \frac{1}{p}\end{pmatrix})$ とおく。このとき次が成立。

(1) $\Psi_i(\tau_0)\in\mathcal{O}_{\mathbb{Q}(\zeta_{2p})}$ $\qquad i=1,2$

(2) $\Theta=\left(\sum_{\nu=0}^{p-1}\zeta_{p^2}^{\nu}\right)\left(\sum_{\nu=0}^{p-1}\Psi_1(\tau_0)^{\nu}\right)\left(\sum_{\nu=0}^{p-1}\Psi_2(\tau_0)^{\nu}\right)$ とおく。

$\Psi_1(\tau_0)\Psi_2(\tau_0)\neq 0$ ならば $\{\Theta^\tau\}_{\tau\in G(L/\mathbb{Q}(\zeta_{2p}))}$ は $L/\mathbb{Q}(\zeta_{2p})$

の正規底である。

証明には[1]と[8]の結果をもちいる。$p=3$のとき $\theta_1(\tau_0)\theta_2(\tau_0)\neq 0$ を日大の福田隆氏に計算していただいた。$k(6)$ の rank 19 の unit group も θ をもちいて構成できる。

References

[1] J. Igusa : Modular forms and projective invariants, Amer J. Math., 89 (1967) 817-855

[2] T. Ito: A construction of normal bases over the Hilbert p-class field of imaginary quadratic fields, to appear in Proc. Japan Acad.

[3] Kersten, I., Michaličtk, J: $\mathbb{Z}_p$-extensions of complex multiplication fields. J. Number Theory 32 (1989) 131-150

[4] I. Kersten, J. Michaličtk : On Vandiver's conjecture and $\mathbb{Z}_p$-extensions of $\mathbb{Q}(\zeta_{p^n})$, J. Number Theory 32 (1989), 371-386

[5] K. Komatsu : Normal basis and Greenberg's conjecture, Math. Ann. 300 (1994), 157-163

[6] K. Komatsu : Construction of normal bases by special values of Siegel modular functions, preprint

[7] M. Kurihara : Notes on the ideal class groups of real

abelian fields, Preprint

[8] G. Shimura: Theta functions with complex multiplication, Duke Math. J., 43 (1976), 673-696.